REMARKS

Applicant requests reconsideration and allowance of the subject patent application in light of the changes above and the remarks that follow.[1] Claims 16-31 are pending, with claim 31 being newly added.

Claim Objection

Claim 27 was objected to on the basis of terminology that was considered to be informal. It is believed that the foregoing amendments to claims 26 and 27 render the objection moot.

Rejection Under 35 U.S.C. § 103(a)

Claims 16-30 were rejected under § 103(a) on the basis of U.S. Publication No. 2002/0069361 to Watanabe et al. in view of U.S. Publication No. 2001/0036301 to Yamaguchi et al.

The Office Action states that the Watanabe publication discloses various embodiments of securing access to a piece of equipment, but does not disclose an embodiment in which an encrypted authentic biometric signature is stored on the piece of equipment to which access is being requested. To this end, therefore, the Office Action refers to the Yamaguchi publication, and specifically its disclosure that registered finger print data for a number of people can be stored on a hard disk device, or the like, in a computer database. The Office Action asserts that it would be obvious to apply this teaching to the public key certificate system of the Watanabe publication. It is respectfully submitted that the logical combination of the

[1] The Office Action contains statements characterizing the claims and related art. Regardless of whether any such statements are specifically addressed herein, Applicant's silence as to these characterizations should not be construed as acceptance of them.

teachings of the two references would not result in the subject matter of the currently pending claims.

In the context of the present invention, the biometric signature, e.g. finger print, that is required for access to a piece of equipment, e.g. a computer, is stored on that piece of equipment. By means of such an arrangement, a single authentication medium, e.g. smart card, can be used to authorize access to a variety of different pieces of equipment, without having to store the biometric signatures for all of those pieces of equipment. Rather, each piece of equipment stores its own set of authorized biometric signatures, and supplies them to the authentication medium at the time that access is requested.

As noted in the background portion of the specification, a concern in this type of arrangement is that a hacker may be able to retrieve biometric signatures stored on the piece of equipment, and thereafter use this information to gain unauthorized access to the piece of equipment. In accordance with a further aspect of the invention, therefore, the biometric signatures are stored on the piece of equipment in an encrypted form. When access to the piece of equipment is requested, the equipment supplies the encrypted biometric signature to the authentication medium, which then decrypts this received authorized signature, and compares it with a newly presented biometric signature, to determine whether access is permitted.

It is respectfully submitted that the Yamaguchi publication does not suggest the differences between the claimed subject matter and the disclosure of the Watanabe publication. Referring to Figure 2 of Yamaguchi et al., cited in the Office Action, the reference discloses that registered finger prints can be stored in the storage unit 414 of the finger print checking device 411. Alternatively, the registered

finger prints can be stored the hard disk drive 425 of a host computer 420, to be downloaded to the storage unit 414, or in an IC card 431, to be transferred to the finger print checking device 411 through the host computer 420. In the context of the Yamaguchi publication, the host computer 420 is not the device, or piece of equipment, to which access is being requested. Rather, the Yamaguchi reference discloses that the finger print checking is carried out in connection with an entrance/exit control system. When the finger print checking device 411 determines that a newly presented finger print matches a registered finger print, it controls the unlocking of the entrance/exit system (paragraph 0041). There is no disclosure that the finger print checking device operates to provide access to the host computer 420.

Rather, the function of the host computer 420 is to support the operation of the finger print checking device 411. Namely, it serves as a storage device for providing registered finger prints to the finger print checking device, or it controls the operation of a card reader 430 to obtain a registered finger print from an IC card 431, and thereafter present it to the finger print checking device. There is no disclosure that the finger print checking device controls access to the host computer 420. Rather, the host computer merely functions to provide registered finger print data to the finger print checking device, so that it can control a different piece of equipment.

A logical application of the teachings of the Yamaguchi publication to the system of the Watanabe publication would be to employ a host computer in connection with the entity that functions to authenticate a biometric signature. Referring to the embodiment of Figure 19 of Watanabe, for example, such an entity would be the Identification Authority (IDA) 320, which stores a template containing authorized finger print data. Yamaguchi teaches that a host computer can be

employed to store, or otherwise provide, the template data to the IDA, rather than storing it within the IDA itself. These combined teachings do not suggest that an authorized biometric signature is stored in the piece of equipment for which access is being requested, e.g. the user device 300. Moreover, neither of the references discloses that an authorized biometric signature is stored in the piece of equipment in an *encrypted* format.

Accordingly, it is respectfully submitted that the Watanabe and Yamaguchi references, whether considered individually or in combination, do not suggest the subject matter of the currently pending claims. Referring to claim 16, for example, they do not suggest a method of securing access to a piece of equipment which includes storing an encrypted version of an authentic biometric signature on the piece of equipment, transmitting the encrypted biometric signature from the piece of equipment to an authentication medium that is separate from the piece of equipment, and decrypting the encrypted authentic biometric signature that is received from the piece of equipment in the authentication medium, for the purpose of verifying a plain biometric signature of a user that has been acquired. For similar reasons, it is respectfully submitted that the references do not suggest the subject matter of independent claims 21 or 26, or any of the claims depending therefrom.

Conclusion

For the reasons set forth above, Applicant respectfully requests allowance of claims 16-31.

In the event that there are any questions concerning this paper, or the application in general, the Examiner is respectfully urged to telephone Applicant's undersigned representative so that prosecution of the application may be expedited.

If additional fees are required for any reason, please charge Deposit Account No. 02-4800 the necessary amount.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: January 25, 2010

By: /James A. LaBarre/
James A. LaBarre
Registration No. 28632

P.O. Box 1404
Alexandria, VA 22313-1404
703 836 6620

Customer No. 21839